

REMARKS

Reconsideration and withdrawal of all grounds of rejection, and allowance of all the pending claims are respectfully requested in light of the above amendments and the following remarks. Claims 1-15 and 17, are now pending herein. Claim 16 has been canceled without prejudice or disclaimer, and new claims 17-18 has been added, claim 17 being supported at least at page 1, line 27 to page 2, line 6; claim 18 is supported by original claim 1 and the disclosure from page 6, line 15, to page 8, line 10.

A replacement FIG. 2 has been submitted herewith to include a showing of the recited control means, and to identify the data-shifted output. Support is found in original claim 1 and the specification at page 2, lines 23-24 and page 8, lines 1-8.

The specification has been updated to correspond with the element numeral of the controls means now shown revised FIG. 2. No new matter has been added.

The Abstract has been amended to overcome the objections in the Office Action. The Abstract is now less than 150 words and any legal phraseology has been removed.

Claim 8 has been amended to overcome the objection thereof on page 2 of the Office Action. Applicant also respectfully submits that claim 15 has been objected to but there is no discussion of the particular issue at hand. Applicant's representative and the Examiner confirmed on a telephone conversation dated June 16, 2008 that claim 15 recites allowable subject matter. Applicant respectfully submits that claim 15 has been rewritten in independent form and is thus allowable.

The cancellation of claim 16 as discussed above overcomes the rejection under 35 U.S.C. §112, second paragraph.

Claims 1-14 and 16 have been rejected under 35 U.S.C. §101 as being alleged to recite non-statutory subject matter. Applicant respectfully traverses this ground of rejection for the reasons indicated herein below.

Applicant has amended claim 1 to clarify the recited hardware structure and purpose. Applicant respectfully submits that the logic circuitry in claim 1 has a practical application in that data is transformed for encryption or decryption and, as shown in FIG. 2, provides a tangible output of a data shifted output having a state "s". The logic circuit according to the present invention transforms data according to, for example, a MixColumns transform and changes the state of the data and stores an output of the changed in a register.

While additional structure might be required to perform other functions to the transformed data (such as the generation of round key function as shown in FIG. 1), the presently claimed invention is directed to a logic circuit with a specific structure and a tangible application and is not merely reciting an algorithm. The MixColumns transformation algorithm is typically used in the Advanced Encryption Standard and the novel structure of the logic circuit as claimed permits an expansion of devices that heretofore could not be used for encryption or decryption.

The presently claimed invention provides a tangible application and is novel and nonobvious, as the configuration of the control means, n multiplication circuits, n logic circuits and, registers and feedback logic that connects the registers to the second input of the logic circuits, for example, for row permutation, results in a tangible output of transformed data having a changed state, and the structure of the recited logic circuitry allows for its incorporation in devices such as smartcards. Applicant respectfully submits

that no there is no known device having the structure as recited in claim 1 for performing the functions recited, and a smartcard having such a logic circuit, thus enabling a smartcard to perform functions heretofore unknown, as the processor and memory resource is very limited in a smartcard. Thus, at least for the reasons discussed, the logic circuit in the present claims is patentable.

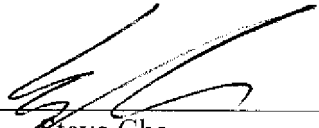
Applicant also respectfully submits that the method recited in claim 18 is also patentable for similar reasons as discussed herein above.

For all the foregoing reasons, it is respectfully submitted that all the present claims are patentable in view of the cited references. A Notice of Allowance is respectfully requested.

Respectfully submitted,

Aaron Waxler
Registration No. 48,027

Date: 6/16/08


By: Steve Cha
Attorney for Applicant
Registration No. 44,069

Mail all correspondence to:
Aaron Waxler, Registration No. 48,027
NXP, B.V.
NXP Intellectual Property Department
M/S41-SJ
1109 McKay Drive
San Jose, CA 95131
Phone: (408) 434-3000
Fax: (408) 474-9081

Fig. 2

